Structure of $\mathbb{Z}^2$ modulo selfsimilar sublattices.*

Roberto Canogar-Mckenzie †
Departamento de Matemáticas,
Facultad de Ciencias, U.N.E.D.,
Madrid 28040, Spain
rcanogar@mat.uned.es

Edgar Martínez-Moro ‡
Dpto. de Matemática Aplicada
Fundamental, Universidad de Valladolid,
Valladolid 47002, Spain
edgar.martinez@ieee.org

February 1, 2008

Abstract

In this paper we show the combinatorial structure of $\mathbb{Z}^2$ modulo sublattices selfsimilar to $\mathbb{Z}^2$. The tool we use for dealing with this purpose is the notion of association scheme. We classify when the scheme defined by the lattice is imprimitive and characterize its decomposition in terms of the decomposition of the gaussian integer defining the lattice. This arise in the classification of different forms of tiling $\mathbb{Z}^2$ by lattices of this type.

Keywords: Association Schemes, Lattices, Tiles, Similarity.

1 Introduction.

A **similarity** σ of **norm** c is a map from $\mathbb{R}^n$ to $\mathbb{R}^n$ such that $\sigma u \cdot \sigma v = cu \cdot v, \quad u, v \in \mathbb{R}^n$. Let Λ be a two-dimensional lattice, a sublattice $\Lambda' \subseteq \Lambda$ is **similar** to Λ if $\sigma(\Lambda) = \Lambda'$. σ is also called a **multiplier** of norm c for Λ. Let us consider now the lattice $\Lambda = \mathbb{Z}[i] \cong \mathbb{Z}^2$ of Gaussian integers, it is a known result [7] that the lattice $\mathbb{Z}^2$ have multipliers of norm c if and only if $c = r^2 + s^2, \quad r, s \in \mathbb{Z}$.

In this paper we shall study the combinatorial structure of sublattices similar to $\mathbb{Z}[i]$ given by $(r+si)\mathbb{Z}[i]$, by studying the quotient $\mathbb{Z}[i]/(r+si)\mathbb{Z}[i]$. From now on, this lattice will be denoted $\mathbb{Z}[i]_{(r+si)}$ for sort. Sublattices selfsimilar to $\mathbb{Z}^2$ have been found useful for recursive constructions of lattices (see [7, 8]) and quotients of this lattices for coding two-dimensional signal constellations in coding theory (see [13, 15]). We define an **association scheme** over the classes in the sublattice. This association scheme is defined by the orbitals of a transitive action (see [4] for a primer on this constructions) . This approach is

*Submitted to Theoretical Computer Science
†This work was realized during a visit of this author to the Department of Algebra and Geometry of the University of Valladolid.
‡This author research is partially supported by the "Junta de Castilla y León" under Project VA-0399 and by DGICYT PB97-901.

the same as defining the association scheme given by Mannheim metric (see [15]) and its well known in coding theory (see [17, " An all purpouse construction"] or [5, 11]). This also arises to different ways of **tiling** $\mathbb{Z}^2$ according the gaussian integer we have chosen.

The organization of the paper is as follows: in the second section we state some of the algebraic preliminaries underlying the paper and also develop a general setting for dealing with schemes derived from quotient lattices. Section 3 shows the construction of the scheme and some of its properties such as the expression of relation matrices. Sections 4 and 5 are devoted to the concept of quotient schemes and its relation with tiling the lattice $\mathbb{Z}^2$. Finally in the conclusions we show some other lines of research.

2 Algebraic Preliminaries

Definition 1. Let X be a finite set. A d-class association scheme is a pair $(X, (R_i)_{i\in I})$, where $I := \{0, 1, \dots, d\}$, such that

1. $(R_i)_{i\in I}$ is a partition of $X \times X$,
2. $\forall i \in I, \exists j \in I$ such that $R_i^t = R_j$,
3. $R_0 := \{(x, x)|x \in X\}$,
4. there are numbers p_{ij}^k such that for any pair $(x, y) \in R_k$ the number of $z \in X$ with $(x, z) \in R_i$ and $(z, y) \in R_j$ equals p_{ij}^k and
5. $p_{ij}^k = p_{ji}^k$ for all $i, j, k \in I$.

Definition 2. An association scheme $(X, (R_i)_{i\in I})$ is called **imprimitive** if some union of relations is an equivalence relation distinct from the trivial ones.

Let Λ be a lattice in n-dimensional space $\mathbb{R}^n$ (i.e. a discrete additive subgroup of $\mathbb{R}^n$). The *automorphism group of* Λ, $\mathrm{Aut}(\Lambda)$, is the set of distance-preserving transformations (or isometries) of the space that fix the origin and take the lattice to it self. Let $\Lambda' \subset \Lambda$ be a sublattice of Λ and $\pi : \Lambda \to \Lambda/\Lambda'$ be the natural projection. We say that the function $s : \Lambda/\Lambda' \to \Lambda$ is a *section of* π if $\pi \circ s$ is the identity. The set $\mathrm{Aut}(\Lambda/\Lambda')$ is composed of the elements of $\mathrm{Aut}(\Lambda)$ that also fix Λ'.

Proposition 3. *We define an association scheme in* Λ/Λ' *in the following way:* $(X_0, Y_0) \in \Lambda/\Lambda' \times \Lambda/\Lambda'$ *and* $(X_1, Y_1) \in \Lambda/\Lambda' \times \Lambda/\Lambda'$ *are in the same relation if and only if there is a* $\sigma \in \mathrm{Aut}(\Lambda/\Lambda')$ *such that for any section* $s : \Lambda/\Lambda' \to \Lambda$ *we have that*

$$\sigma(s(Y_0 - X_0)) \equiv s(Y_1 - X_1) \pmod{\Lambda'}.$$

Proof. 1. By the definition of the relations, condition 1 is satisfied.

2. The pair (X,Y) is in the same relation as (Y,X) because $-(s(Y-X)) \equiv s(X-Y)(\mod \Lambda')$. Note that the multiplication by -1 is an element of $\mathrm{Aut}(\Lambda/\Lambda')$. It follows that $R_i^t = R_i$ for all $i \in I$. Then we say that the association scheme is symmetric.

3. For all $X, Y \in \Lambda/\Lambda'$, (X,X) and (Y,Y) are in the same relation. Thus $R_0 \supset \{(X,X) \mid X \in \Lambda/\Lambda'\}$. If (X,Y) is in the same relation than (Z,Z), then $\exists \sigma \in \mathrm{Aut}(\Lambda/\Lambda')$ such that:

$$\sigma(s(Y-X)) \equiv s(Z-Z) \equiv s(0)(\mod \Lambda').$$

Then

$$\sigma(s(Y-X)) \in \Lambda' \Rightarrow s(Y-X) \in \Lambda' \Rightarrow Y-X=0$$

We conclude that $R_0 = \{(X,X) \mid X \in \Lambda/\Lambda'\}$.

4. Let $(X_t, Y_t) \in R_k$ and let

$$E_t = \{Z \in \Lambda/\Lambda' \mid (X_t, Z) \in R_i \text{ and } (Z, Y_t) \in R_j\},$$

for $t = 0,1$. Then there is a $\sigma \in \mathrm{Aut}(\Lambda/\Lambda')$ such that for any section $s : \Lambda/\Lambda' \to \Lambda$ we have that

$$\sigma(s(Y_0 - X_0)) \equiv s(Y_1 - X_1)(\mod \Lambda).$$

Let $f : \Lambda \to \Lambda$ be defined as $f(x) = \sigma(x - s(X_0)) + s(X_1)$. Then $\pi(f(s(Y_0))) = Y_1$. We will prove that $\#E_0 \geq \#E_1$. For every $Z \in E_0$ we can check that $(X_1, \pi(f(s(Z)))) \in R_i$ and also that $(\pi(f(s(Z))), Y_1) = (\pi(f(s(Z))), \pi(f(s(Y_0)))) \in R_j$. This means that $Z \in E_1$. Then $\pi \circ f \circ s$ is a function from E_0 to E_1. We still need to show that this function is injective. Let $Z_0, Z_1 \in \Lambda/\Lambda'$ and let us assume that

$$\begin{gathered}\pi \circ f \circ s(Z_0) - \pi \circ f \circ s(Z_1) = 0 \Rightarrow \pi(\sigma(s(Z_0)) - \sigma(s(Z_1))) = 0 \Rightarrow \\ \sigma(s(Z_0) - s(Z_1)) \in \Lambda' \Rightarrow s(Z_0) - s(Z_1) \in \Lambda' \Rightarrow \\ \pi(s(Z_0)) - \pi(s(Z_1)) = 0 \Rightarrow Z_0 = Z_1.\end{gathered}$$

5. By the symmetry of the association scheme we deduce that $p_{ij}^k = p_{ji}^k$.

□

2.1 The Bose-Mesner algebra

This definition in terms of relations allows us a much more convenient way to describe association schemes in terms of algebras.

From now on we will suppose that X has n ordered elements: $X = \{x_1, \dots, x_n\}$. If we have an association scheme $(X, (R_i)_{i\in I})$, the family $(A_i)_{i\in I}$ of non-zero $n \times n$ $(0,1)$-matrices will denote the adjacency matrices of the corresponding relations (the rows and columns of A_i, and all matrices of size $n \times n$ on what follows, are indexed by X in the specified order). Now we can reformulae the conditions in terms of matrices.

1. $\sum_{i\in I} A_i = J$,
2. $\forall i \in I, \exists j \in I$ such that $A_i^* = A_j$ (where A_i^* is the adjoint of A_i),
3. $A_0 = I_n$,
4. $A_iA_j = \sum_{k\in I} p_{ij}^k A_k$ $(i,j \in I)$ and
5. $A_iA_j = A_jA_i$.

By conditions 1 to 4, $\{A_i\}_{i\in I}$ form a base (as a vector space over $\mathbb{C}$) of a subalgebra in $M_n(\mathbb{C})$, so the algebra has dimension $d+1$. By 5 this subalgebra is commutative. This algebra, $\mathcal{A}$, is called the *Bose-Mesner* algebra of the association scheme.

3 Definition of the scheme

Consider the lattice of Gaussian integers $\mathbb{Z}[i]$ and the sublattice $L = \mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ the set of Gaussian integers modulo $\alpha\mathbb{Z}[i]$ which is similar to $\mathbb{Z}[i]$. The *norm* of an element $\alpha \in \mathbb{Z}[i]$ is just $N(\alpha) = \alpha \cdot \bar{\alpha}$. The *units* are the elements of norm 1. Clearly multiplication in L by an element on the group of units of the Gaussian integers $\mathcal{G} = \langle i \rangle$ (i is the imaginary unit) is an isometry fixing the origin (from now on we shall refer to them as rotations) , and also we shall denote the group of translations by $\mathcal{T}$.

In the following discussion we will need some notation on permutation groups acting on finite sets. For an reference on this topic see [1, 4]. For a given permutation group $\mathcal{G}$ of elements of a finite set X we denote the orbit of an element $x \in X$ as $(\mathcal{G})(x) = \{xg \mid g \in \mathcal{G}\}$. Two orbits are either identical or disjoint. We denote by $\mathcal{O}(\mathcal{G} \mid X)$ the set of all the orbits of the action. We denote the stabilizers by $\mathcal{G}_x = \{g \in \mathcal{G} \mid x = xg\}$. It is well known the relation between orbits and stabilizers given by:

$$\begin{array}{ccc} \Big(\mathcal{G}\Big)(x) & \rightarrow & \mathcal{G}/\mathcal{G}_x \\ xg & \mapsto & \mathcal{G}_x g \end{array}$$

The action is *transitive* if there is just one orbit. If the action is transitive, a *congruence* is a $\mathcal{G}$-invariant equivalence relation on X. We say the action is *imprimitive* if has a non-trivial equivalence.

Consider now the *semi direct* product of both groups $\mathcal{H} = \mathcal{G} \ltimes \mathcal{T}$. Roughly speaking we will also denote by $\mathcal{H}$ the permutation group on L generated by the permutation $(\alpha \mapsto i\alpha)$ and the translations in $\mathcal{T}$. It is clear that $\mathcal{H}$ acts transitively on L.

Consider the orbits of the action:

$$\mathcal{H} \times (L \times L) \rightarrow (L \times L)$$

induced by the action of $\mathcal{H}$ on L. They are called *orbitals* and they are the relations of an association scheme [4]. Since $\mathcal{H}$ is a transitive permutation

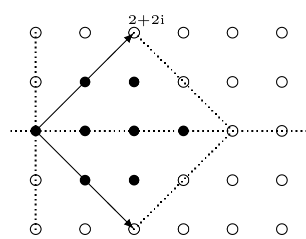
group, if we take G_0 (i.e. those permutations that fix 0), it is well known that we have the coset decomposition: $\mathcal{H} = \big(G_0\big)(p_0) \cup \cdots \cup \big(G_0\big)(p_t)$, where p_i is the permutation transforming 0 in some complex number β belonging to the coset. Therefore orbits can be rewritten as:

$$(x, y) \in R_k \Leftrightarrow x - y \in \big(G_0\big)(p_k) \tag{1}$$

In our case $G_0 = \mathcal{G}$.

Example 4. *Consider the sublattice $\mathbb{Z}[i]_{(2+2i)}$. We can give a system of representants in the fundamental region given in the figure 1.*

Figure 1: $\mathbb{Z}[i]_{(2+2i)}$



The orbitals of the previous action are given by the cosets (see (1)):

$$\begin{array}{ll} \big(G_0\big) \cdot (0) = \{0\} & \big(G_0\big) \cdot (1) = \{\pm 1, \pm i\} \\ \big(G_0\big) \cdot (2) = \{2\} & \big(G_0\big) \cdot (1+i) = \{1+i, 1-i\} \end{array}$$

Which allows us construct the relations in the association scheme.

Theorem 5. *The association scheme $(X, (R_i)_{i \in I})$ with $X = L$ and $(R_i)_{i \in I}$ defined by the orbitals of the action above is primitive if and only if α is a prime in $\mathbb{Z}[i]$.*

Proof. Suppose that α is not a prime in $\mathbb{Z}[i]$, i.e. $\alpha = \alpha_1 \cdot \alpha_2$. Then it is clear that the equivalence in L given by the quotient $L/[\mathbb{Z}[i]/\alpha_1\mathbb{Z}[i]] \subset L$ is $\mathcal{G}$-invariant, and therefore the action is imprimitive, hence by proposition 2.9.3 in [3] the association scheme is imprimitive.

Conversely, if α is prime then is a well known fact in number theory (see [12]) that either it is $1+i$ multiplied by an unit or:

1. $N(\alpha) = p \equiv 1 \mod 4$, p an odd prime, and in this case the lattice L has p points, and clearly $\mathcal{T} \cong \mathbb{Z}_p$.

2. $\alpha = p \in \mathbb{Z}$ and $p \equiv 3 \mod 4$, in this case L can be represented as $\mathbb{Z}_p[i]$, and therefore has p^2 points and $\mathcal{T} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

In the case $1+i$ it is obvious that the scheme is primitive, in the other two cases we have that the estabiliser of any point β in the lattice is given by the group of rotations around the point (i.e. $G_\beta = t_\beta \mathcal{G}(t_\beta)^{-1}$, where t_β is the translation of vector β). It is clear that in both cases above there is no group between $\mathcal{G}_\beta < \mathcal{H}$ since the group generated by a single element in $\mathcal{T}$ and the group $\mathcal{G}_\beta$ is $\mathcal{H}$ (See remark below for a further explanation). Therefore the estabiliser is maximal, and by theorem 1.9 in [4], the action is primitive, and so is the association scheme. □

Remark 6. Indeed, if G_β are the rotations around the point β and we add a new rotation around other point, say $\beta' \neq \beta$, then the group generated contains all rotations around β'. Moreover, the composition of the i rotation arund one of the points, and i^3 around the other is a translation. So in the proof above we can suppose that we always add one translation.

When there is a prime number of points, it is clear that a single translation generates the group $\mathcal{T}$ since is cyclic of prime order. In the case $\mathcal{T} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ a translation t and the translation $i^{-1} \circ t \circ i$ are independent and generate the whole group $\mathcal{T}$. In remark 7 we will show the relation of this facts with the construction of constellations representing $GF(p)$ and $GF(p^2)$ respectively.

The association scheme defined is a **translation asociation scheme**, and in the case of a prime number of points (i.e. $|X|$ is a prime) is a **cyclotomic** scheme (see [3] for the definitions).

Remark 7. The two constructions we present below are used to construct two-dimensional modulo metrics (in particular Mannheim distance) for coding theory (for further details see [13, 14, 15]).

a) Let $\pi \in \mathbb{Z}[i]$ be an element whose norm is a prime integer p, and $p \equiv 1 \mod 4$. It is well known (Fermat's two square theorem) that p can be written as:

$$p = a^2 + b^2 = \pi\bar{\pi} \text{ where } \pi = a + ib \text{ (not unique).}$$

If we denote by $\mathbb{Z}[i]_\pi$ the set of Gaussian integers modulo π, we define the modulo function $\nu : \mathbb{Z}[i] \to \mathbb{Z}[i]_\pi$ associating to each class in $\mathbb{Z}[i]_\pi$ its representant with smallest norm :

$$\nu(\xi) = r \text{ where } \xi = q\pi + r \text{ and } \|r\| = \min\{\|\beta\| \mid \beta = \xi \text{mod} \pi\} \quad (2)$$

This can be done because $\mathbb{Z}[i]$ is and Euclidean domain. The quotient q can be calculated as $[\frac{\alpha\bar{\pi}}{p}]$ where $[x]$ denotes the Gaussian integer with closest real and imaginary part to x. The quotient q can be calculated as $[\frac{\alpha\bar{\pi}}{p}]$ where $[x]$ denotes the Gaussian integer with closest real and imaginary part to x.

Taking the carrier set of $GF(p)$ as $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$, we can restrict to $GF(p)$ the application ν so that it induces an isomorphism $\nu : GF(p) \to \mathbb{Z}[i]_\pi$ given by:

$$\text{For } g \in GF(p) \quad \nu(g) = g - [\frac{g\bar{\pi}}{p}]\pi$$

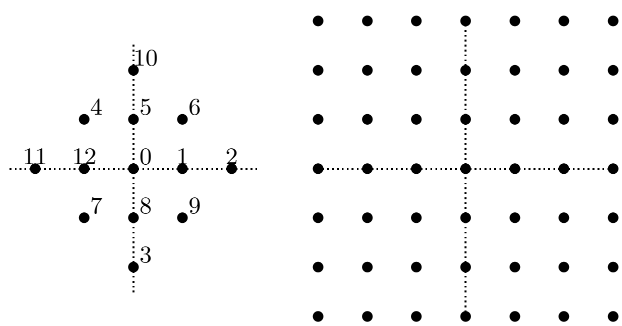
So $GF(p)$ and $[i]_\pi$ are mathematically equivalent and we shall use from now on that carrier set for a sort notation.

b) In the case $p \equiv 3 \mod 4$ $\pi = p \in \mathbb{Z}$ and the isomorphism above does not apport any relevant information over $GF(p)$. For this type of primes -1 is a quadratic non residue of p, hence we get the following isomorphism between $GF(p^2)$ and $\mathbb{Z}_p[i]$ where :

$$\mathbb{Z}_p[i] = \Big\{ k + il \mid k, l \in \big\{ \frac{-(p-1)}{2}, \dots, -1, 0, 1, \dots, \frac{(p-1)}{2} \big\} \Big\}$$

Example 8. *Consider $\mathbb{Z}[i]_{3+2i}$ and $\mathbb{Z}_7[i]$, given by the carrier sets defined as in the previous remark . We have an alternative pictorial representation of them to usual one derived as in example 4 given by figure 2. This representation is more suitable for showing the symmetries and rotations within the fundamental region. For the association scheme of this constellations of points see example 10.*

Figure 2: $GF(13)$ as $\mathbb{Z}[i]_{3+2i}$ and $GF(7^2)$ as $\mathbb{Z}_7[i]$



3.1 Matrix expression of the algebra

In this section we develop and easy way for describing the matrices of the Bose-Mensner algebra associated to this sublattices in terms of circulant matrices.

Definition 9. Let M be a $n \times n$ matrix and let $\{a_i\}_{i=0,\dots,n-1}$ be the first row of M. Then M is **circulant** if:

$$M_{ij} = a_{(i-j) \mod n}, \quad i, j = 0, 1, \dots, n$$

First we shall insight in the case of a prime number of points p. In this case we have that the translations $\mathcal{T}$ are a clyclic group of prime order, hence, if we

choose an element generating $\langle t\rangle = \mathcal{T}$, any element $l \in L$ can be rewritten as $l = t^j(0), \quad 0 \leq j \leq p-1$, and choosing the order given by j for the points in the scheme it is clear that the matrices R_i are circulant since t is an isometry.

Example 10. *In the case $L = \mathbb{Z}[i]_{3+2i}$ of the previous example the orbits can be described knowing the cosets:*

$$\begin{array}{rr} \big(G_0\big)\cdot(p_0) = \{0\} & \big(G_0\big)\cdot(p_1) = \{1,5,12,8\} \\ \big(G_0\big)\cdot(p_2) = \{6,4,7,9\} & \big(G_0\big)\cdot(p_3) = \{2,10,11,3\} \end{array}$$

And if we choose the translation given by adding 1 to each point for ordering the relations (the usual order for $GF(p)$), then they are given by:

$$\begin{array}{ll} D_0 = [1,0,0,0,0,0,0,0,0,0,0,0,0] & D_1 = [0,1,0,0,0,1,0,0,1,0,0,0,1] \\ D_2 = [0,0,0,0,1,0,1,1,0,1,0,0,0] & D_3 = [0,0,1,1,0,0,0,0,0,0,1,1,0] \end{array}$$

Note that each matrix D is represented only by its first row since they are circulant. Moreover, as usual we shall collect al the information in a single matrix as:

$$[0,1,3,3,2,1,2,2,1,2,3,3,1]$$

Remark 11. The eigenvalues of a circulant matrix are computed easily (see [2]) as sums of roots of the unit, and hence, so are the eigenvalues of the scheme (see [15]).

In the case of a non-prime number of points, we have a slightly modified construction based on the decomposition of $\mathcal{T}$ as the direct product of cyclic subgroups. The idea is the same as in the previous example, and now the matrices are circulant in blocks given by the clyclic subgroups. We shall illustrate this idea with an example.

Example 12. *Consider $L = \mathbb{Z}[i]_{(2+2i)}$ as in example 4. Consider the isomorphism given by:*

$$\begin{aligned} L = \mathbb{Z}[i]_{(2+2i)} &\xrightarrow{\sim} \mathbb{Z}_4 \times \mathbb{Z}_2 \\ 1 &\mapsto (1,0) \\ 1+i &\mapsto (0,1) \end{aligned}$$

Consider now the elements in the order given by

$$(0,0),(1,0),\ldots,(3,0),(0,1),(1,1),\ldots,(3,1)$$

The relation matrices can be expressed now as block circulant matrices:

$$D_i = \begin{bmatrix} D_{i1} & D_{i2} \\ D_{i2} & D_{i1} \end{bmatrix} \quad i = 0,\ldots,3$$

Where each block is a circulant matrix. The relations in example 4 can be represented in the same fashion as previous example:

$$[0,1,2,1|3,1,3,1]$$

where $|$ means the division of the blocks.

Proposition 13. *The relation matrices can be expresed as block-circulant matrices, where each block is also a circulant matrix.*

Proof. It follows directly from the reasoning above, i.e. the decomposition of the group of translations in a product of cyclic groups. □

4 Quotient schemes

We introduce in this section the concept of quotient scheme. For an account on this topic see [3]. Suppose a set of indices $\widetilde{0}$, and let us define the equivalence relation $\sim$ among the set of indices of the relations in the scheme $(X, \mathcal{R})$ as follows:

$$a \sim b \text{ if } p^i_{ab} \neq 0 \text{ for some } i \in \widetilde{0}$$

As usual $\widetilde{0}$ is the class of 0 and we write $\widetilde{a}$ for the relation containing a.

Definition 14. We define a **quotient scheme** $(\tilde{X}, \tilde{\mathcal{R}})$ of $(X, \mathcal{R})$ with respect to $\tilde{0}$ as the association scheme whose point set is the set $\tilde{X}$ of equivalence classes on X, and whose relations are $\tilde{R}_{\tilde{i}}$, with

$$\tilde{R}_{\tilde{i}} = \{(\tilde{x}, \tilde{y}) \mid \text{ for } x \in \tilde{x}, y \in \tilde{y} \text{ we have } (x, y) \in R_i \text{ with } i \in \tilde{\imath}\}$$

Proposition 15. *If the scheme defined on L is imprimitive we can define a quotient scheme where $\tilde{0}$ is given by the classes of some of the elements divisors of* 0.

Proof. It is obvious by the first part of the proof of theorem in 5. □

Example 16. *Consider $L = \mathbb{Z}[i]_{(2+2i)}$ as in examples 4 and 12, and consider the relation given by $\tilde{0} = \{0, 2\}$. With the notation in example 12 we have:*

$$\widetilde{(0,0)} = \{(0,0),(2,0)\} \quad \widetilde{(1,0)} = \{(1,0),(3,0)\}$$
$$\widetilde{(0,1)} = \{(0,1),(2,1)\} \quad \widetilde{(1,1)} = \{(1,1),(3,1)\}$$

And the relation matrix in the order given by $\widetilde{(0,0)}, \widetilde{(1,0)}, \widetilde{(0,1)}, \widetilde{(1,1)}$ is:

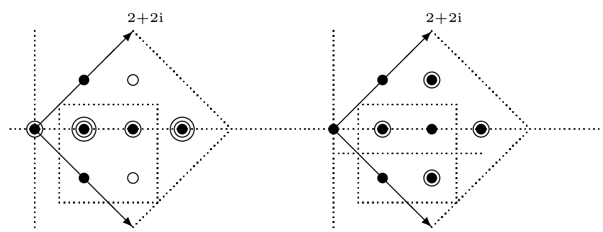
$$[0, 1, 2, 1]$$

Remark 17. Indeed, in the previous example, the translations are given by the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, (this can be seen also because $2 = (1+i)(1-i)$ is not a gaussian prime) and admits a further quotient scheme given by:

$$\widetilde{\widetilde{(0,0)}} = \{\widetilde{(0,0)}, \widetilde{(0,1)}\} \quad \widetilde{\widetilde{(1,0)}} = \{\widetilde{(1,0)}, \widetilde{(1,1)}\}$$

This corresponds with the identifications in the figure 3.

Figure 3: Quotients of $\mathbb{Z}[i]_{(2+2i)}$



Remark 18. Note that following [3, pp.52], if we let $A = \{a \mid p^0_{aa} = 1\}$ then for each $a \in A \setminus \{0\}$ we find a involution $\sigma_a : x \mapsto \bar{x}, \quad (x, \bar{x}) \in R_a$, and if we set $\sigma_0 = 1$ them $\sigma_a \sigma_b = \sigma_b \sigma_a = \sigma_c$ where c is determined by $p^c_{ab} \neq 0$. A clearly has the structure of an elementary abelian 2-group.

Remark 19. There is a sort of Jordan-Hölder theory relating the facts above that for our example we can summarize as follows:

$$\begin{array}{c} \mathbb{Z}_{(2+2i)} \\ \bigcup \\ \mathbb{Z}_{(2)} \\ \bigcup \\ \mathbb{Z}_{(1+i)} \end{array}$$

$\mathbb{Z}_{(\alpha)}$	$\mathcal{T}$	$\{a \mid p^0_{aa} = 1\}$
$\mathbb{Z}_{(2+2i)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$0, 2$
$\mathbb{Z}_{(2)}$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\widetilde{(0,0)}, \widetilde{(0,1)}$
$\mathbb{Z}_{(1+i)}$	$\mathbb{Z}_2$	$\widetilde{\widetilde{(0,0)}}$

5 Relation with tilings

Up to now we have shown that we have tree types of primitive sublattices, depending on the gaussian prime defining it, this arises to three different forms of tiling the whole $\mathbb{Z}^2$.

- With tiles of type $\mathbb{Z}[i]_{(1+i)}$;
- with tiles of type $\mathbb{Z}[i]_{(a+bi)}$ where $N(a+bi) = p$ an odd prime $\equiv 1 \mod 4$;
- with tiles of type $\mathbb{Z}_p[i]$; p an odd prime $\equiv 3 \mod 4$.

Indeed this has a close relationship with the well known fact in number theory given by the criterion for representability of a number N by the sum of two squares which says that any prime factor of N which is of the form $4k + 3$ must divide N to an even power exactly [9]. In our setting this means (as we have seen) that the regions defined by an integer of norm p^n, p a prime of this type must have p^{2n} points. This fact relates each prime in the factorization of the norm N with a type of the primitive tiles above.

In the three cases above the boundary of the Voronoi cell of the sublattice $\alpha\mathbb{Z}[i]$ does not contain any extra points of $\mathbb{Z}^2$ so following notation in [3] we

called such sublattices *clean*. Hence, in the case of clean sublattices we can find a complete set of representatives of the non-zero classes within the region bounded by α and $i \cdot \alpha$. Moreover they are clean if there is an odd number of points [3], i.e. there is no an involution (see remark 18), so it follows directly the following result (as expected):

Corollary 20. *Any quotient of a clean sublatice L defined as in section 3 is also clean.*

Remark 21. The primitive schemes above are the finest translation schemes from our setting. Recall that in the schemes defined for an odd prime we have in all cases all orbits are of size 4, but the schemes are not pseudocyclic (see [3] for a definition) since $\sum_i p_{ii}^k \neq 3$. We can go a bit farther with the following result of Rao, Ray-Chau and Singhi [3, pp.52 ii],[16]: they state that the finest translation association scheme for a set of odd order is pseudocyclic and the other translation schemes for the same set can be derived from this one by merging classes. In the case of the schemes in this paper the scheme they recall is the one generated by the $1, i^2$ rotations an the translations, and clearly each relation of our scheme arises from the merging of two relations of it.

6 Conclusions

We have study the combinatorial structure of the association schemes derived from sublattices given by $\mathbb{Z}[i]/(r+si)\mathbb{Z}[i]$. As we have seen, there are close connections of this type of lattices with coding theory, recursive construction of lattices and self-similar lattices [3, 13, 14, 15]. In the study of the scheme defined plays a central role the factorization of the gaussian integer $(r+si)$ and also the factorization of the order of the group of translations $\mathcal{T}$ (i.e. the number of points in the sublattice). We have characterize the primitive cases and also identify the cases where the Voronoi cell is clean both from a combinatorial point of view and from a number theoretical one. We can see the primitive case as the finest tiles of the lattice $\mathbb{Z}^2$ and they are useful in coding two dimensional signal spaces with Mannheim metric [13]. We have also shown how derive an easy expresion of the matrices defining the relations in the schemed based in thier circulant structure. A similar study can be done with hexagonal schemes an hexagonal metric based on Einsestein-Jacobi integers [15] and will be shown elsewhere. Future trends of investigation point toward classifying the partition designs derived from this type of association schemes [6].

References

[1] J.L. Alperin , R.B. Bell, Groups and representations, Graduate Text in Mathematics 162,(1995) Springer Verlag.

[2] N. Biggs, Algebraic Graph theory, 2nd. edition (1993), Cambridge University Press.

[3] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance regular graphs. Springer Verlag.

[4] P.J. Cameron, Permutation groups. London Mathematical Society (1999). Cambridge University Text.

[5] P. Camion, Codes and association schemes: basic properties of association schemes relevant to coding. In: Handbook of coding theory vol. II. Edited by V.S. Pless and W.C. Huffman. Elsevier Science (1998).

[6] R. Canogar-Mckenzie, E. Martínez-Moro, Partition designs for two dimensional modulo metrics. Preprint in preparation.

[7] J.H. Conway, E.M. Rains, N.J.A. Sloane, On the existence of similar sublattices. Canadian Journal of Mathematics (1999), **6**, 1300–1306

[8] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer Verlag, 3rd. ed, 1998.

[9] H. Davenport, The higher arithmetic. 6th. edition. (1993). Cambridge University Press.

[10] P. Delsarte, An algebraic approach to the association schemes of coding theory., Technical report, Philips Research Laboratory (1973)

[11] P. Delsarte,V.I. Levenshtein, Association schemes and coding theory. IEEE Trans. on Inf. Theory, vol. 44, 6, (1998), 2477–2504.

[12] G.H. Hardy, E.M. Wright, An introduction to the theory of numbers. Oxford Science Publications, 5th. edition (1979).

[13] K. Huber, Codes over Gaussian integers., IEEE Trans. on Inf. Theory, **40**(1) (1994), 207–216.

[14] K. Huber, The Mac Williams Theorem for Two-dimensional modulo metrics, AAECC, **8**(1) (1997), 41–48.

[15] E. Martínez-Moro, F.J. Galán-Simón, M.A. Borges-Trenard, M. Borges-Quintana, Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics. Criptography and Coding. Lecture Notes in Computer Science **1746** (1999), Springer Verlag. 45–55

[16] S.B. Rao, D.K. Ray-Chaudry, N.M. Shinghi, On imprimitive association schemes, in: Combinatorics and applications- Proc. of the Seminar on Combinatorics and Applications in honour of Prof. S.S. Shrikhande. Indian Statist. Inst. Calcuta (1984), 273–291.

[17] P. Solé, On the parameters of codes for the Lee and modular distance. Discrete Mathematics 89 (1991), 185–194.